CLAIMS

What is claimed is:

1. A method for detecting systematic attacks and unauthorized attempts to access a host computer, said host computer having an event list containing time-stamped records for each attempt to login or logon to the host computer, said records including user detail information such as a user name, said event list having an earliest event and a latest event with the time there between being a scan time, said method comprising the steps of:

establishing a float period length having a finite time duration;

establishing a float period at an initial position, said float period having a start time and an end time, said end time being equal to said start time plus said float period length, wherein said start time is initially equal to a time stamp value of said earliest event in said event list;

counting a number of events in said event list which fall within said current float period;

responsive to said count exceeding a threshold, producing a violation message and jumping said float period by setting said start time to be equal to a time stamp value of an event in said event list immediately following said float period end time, otherwise advancing said float period by a single event by setting said start time to a time stamp value of an event in said event list immediately following said start time; and iterating said steps of counting, producing a violation message and jumping said float period and single-event advancing of said float period until said float period end time exceeds a time stamp value of said latest event in said event list.

2. The method as set forth in Claim 1 wherein said step of producing a violation message comprises creating a report viewable by a system administrator.

3. The method as set forth in Claim 1 wherein said step of advancing by a single-event the float period further comprises producing a warning message if said count is equal to or greater than 1.

4. The method as set forth in Claim 1 further comprising a step of producing said event list by accessing at least one host computer system audit file containing said events, extracting said events from said audit file, and producing said event list.

5. The method as set forth in Claim 1 wherein said step of counting a number of events in said event list comprises counting only events for a single user.

6. A computer readable medium encoded with software for detecting systematic attacks and unauthorized attempts to access a host computer, said host computer having an event list containing time-stamped records for each attempt to login or logon to the host computer, said records including user detail information such as a user name, said event list having an earliest event and a latest event with the time there between being a scan time, said causing

said host computer to perform the steps of:

establishing a float period length having a finite time duration;

establishing a float period at an initial position, said float period having a start time and an end time, said end time being equal to said start time plus said float period length, wherein said start time is initially equal to a time stamp value of said earliest event in said event list;

counting a number of events in said event list which fall within said current float period;

responsive to said count exceeding a threshold, producing a violation message and jumping said float period by setting said start time to be equal to a time stamp value of an event in said event list immediately following said float period end time, otherwise advancing said float period by a single event by setting said start time to a time stamp value of an event in said event list immediately following said start time; and

iterating said steps of counting, producing a violation message and jumping said float period and single-event advancing of said float period until said float period end time exceeds a time stamp value of said latest event in said event list.

7. The computer readable medium as set forth in Claim 6 wherein said software for producing a violation message comprises software for creating a report viewable by a system administrator.

8. The computer readable medium as set forth in Claim 6 wherein said software

for advancing by a single-event the float period further comprises software for producing a warning message if said count is equal to or greater than 1.

9. The computer readable medium as set forth in Claim 6 further comprising software for producing said event list by accessing at least one host computer system audit file containing said events, extracting said events from said audit file, and producing said event list.

10. The computer readable medium as set forth in Claim 6 wherein said software for counting a number of events in said event list comprises software for counting only events for a single user.

11. A system for detecting systematic attacks against a host computer by analyzing an event list of attempted log-ons and accesses, said event list having a plurality of events comprised of time stamps and user names, said event list having an earliest event and a latest event, said system comprising:

a float period manager for advancing a float period from an initial position to a plurality of subsequent positions, said initial position having a float period start time equivalent to said earliest event time stamp and a float period end time equal to said start time plus a float period length, said float period being adapted to jump the float period to a subsequent position such that said start time is equivalent to a time stamp of an immediately subsequent event following said end time, and also being adapted to advance said float period to a subsequent position by a single event such that said start time is equivalent to a time stamp of an immediately subsequent event following said start time;

an event counter for determining an event count within a given position of said float period; and

an evaluator for comparing said event count to a violation threshold, and responsive to said count exceeding said threshold, producing a violation message and causing said float period manager to jump said float period to a subsequent position, otherwise causing said float period manager to advance said float period by a single-event to a subsequent position, until said float period end time exceeds a time stamp of said latest event in the event list.

12. The system as set forth in Claim 11 wherein said event counter is adapted to count events associated with a single user.

13. The system as set forth in Claim 11 wherein said evaluator is adapted to produce a report viewable by a system administrator.

14. The system as set forth in Claim 11 wherein said evaluator is adapted to produce a warning message if said event count exceeds 1 and is less than or equal to said violation threshold.

15. The system as set forth in Claim 11 further comprising an event list producer for producing said event list from one or more audit files.